Bedingungen für die Teilnahme am Mastercard Identity Check™-Verfahren für MLP Kreditkarten mittels einzelumsatzbezogener Transaktionsnummer

1. Geltungsbereich

Der Inhaber einer MLP Kreditkarte und die MLP Banking AG (nachfolgend „Bank“ genannt) vereinbaren, dass die folgenden Bedingungen für die Teilnahme am Mastercard Identity Check™-Verfahren in den zwischen den Parteien bestehenden Kreditkartenvertrag einbezogen werden. Diese Bedingungen gelten für den Einsatz der MLP Kreditkarte im Rahmen des Mastercard Identity Check™-Verfahrens zusammen mit einer auf den Einzelumsatz bezogenen Transaktionsnummer (TAN).
Diese Sonderbedingungen gelten ergänzend zu den „Vertragsbedingungen für die MLP Kreditkarten“ und den Allgemeinen Geschäftsbedingungen von MLP. Im Falle eines Widerspruchs zwischen den „Vertragsbedingungen für die MLP Kreditkarten“ gehen diese den Sonderbedingungen vor.
Der Wortlaut dieser Bedingungen kann beim MLP Kundenservice, Telefon +49 (0) 6222 • 3169 •4000 angefordert, unter der Internetadresse der Bank (www.mlp.de) oder beim MLP Berater eingesehen und angefordert werden. Der Karteninhaber kann jederzeit die Übermittlung dieser Bedingungen in Textform von der Bank verlangen.

2. Mastercard Identity Check™

Mastercard Identity Check™ ist ein Verfahren zur gesicherten Authentifizierung, das dazu dient, sicherzustellen, dass eine Internetzahlung bei einer Kartenakzeptanzstelle, die an diesem Verfahren teilnimmt, auch tatsächlich vom Karteninhaber veranlasst wurde und die Karte nicht zu Unrecht belastet wird. Hierzu bestätigt der Karteninhaber beim Bezahlvorgang gegenüber einem Dienstleister der Bank mittels Eingabe einer auf den Einzelumsatz bezogenen Transaktionsnummer (TAN) oder durch Freigabe in einer durch die Bank bereitgestellten App, dass er die Zahlung beauftragt. Die TAN wird dann an ein für den SMS-Empfang geeignetes Endgerät (z. B. Mobiltelefon) oder an eine auf dem Endgerät des Karteninhabers installierte, durch die Bank bereitgestellte App übermittelt.

3. Registrierung

3.1. Erforderliche Daten und technische Anforderungen

Um sich zur Teilnahme an diesen Authentifizierungsverfahren zu registrieren, benötigt der Karteninhaber

- seine Kreditkartennummer,
- ggf. weitere persönliche Daten, die während der Registrierung abgefragt werden, und
- ein Endgerät (z. B. Mobiltelefon) mit der Möglichkeit des SMS-Empfangs (nachfolgend „Mobiltelefon“ genannt) („SMS-Verfahren“) oder
- ein anderes unterstütztes Endgerät (z. B. Smartphone/Tablet) mit der Möglichkeit der Nutzung der durch die Bank bereitgestellten App („App-Verfahren“).

Die Bank behält sich das Recht vor, nicht beide vorgenannten Verfahren anzubieten oder sie durch ein anderes oder mehrere andere Verfahren zu ersetzen. Die Registrierung ist auf der Internetseite der Bank möglich. Optional kann die Registrierung während eines Bezahlvorgangs bei einem teilnehmenden Internethändler durch die Bank initiiert werden.

3.2. Registrierungsprozess für das SMS-Verfahren

Hierbei legt der Karteninhaber die Rufnummer seines Mobiltelefons fest, an das künftig die zur Zahlungsfreigabe erforderlichen TANs übermittelt werden sollen. Bei der Erstregistrierung für das Verfahren wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber vor der Hinterlegung der Mobilfunknummer und der persönlichen Angaben auf der Internetseite von MLP einmalig eingeben. Danach ist das SMS-Verfahren für die Nutzung zur gesicherten Authentifizierung freigeschaltet.

3.3. Registrierungsprozess für das App-Verfahren
Das App-Verfahren setzt voraus, dass der Karteninhaber die von MLP bereitgestellte App auf seinem Endgerät installiert und mit seiner Kreditkarte per Aktivierungscode verknüpft. Die bei erstmaliger Nutzung der App erzeugte Kennung (die „virtuelle Handynummer“) ist bei der Registrierung anzugeben. Bei der Registrierung für das Verfahren wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber vor der Hinterlegung der virtuellen Handynummer auf der Internetseite der Bank einmalig eingeben. Danach ist das App-Verfahren für die Nutzung zur gesicherten Authentifizierung freigeschaltet und der Karteninhaber hat die Möglichkeit, mittels der von der Bank bereitgestellten App die TANs zu empfangen oder innerhalb der App freizugeben.

3.4. Weitere Informationen
Die Bank wird den Karteninhaber niemals per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern.

4. Gesicherte Authentifizierung einer Mastercard Identity Check™-Zahlung

4.1. SMS-Verfahren:
Sobald eine Mastercard Identity Check™-Transaktion veranlasst wird, erhält der Karteninhaber eine SMS-Benachrichtigung mit Transaktionsdetails und die pro Transaktion generierte TAN auf sein Endgerät zugestellt. Durch Eingabe der erhaltenen TAN im Kaufprozess wird die Transaktion bestätigt und der Karteninhaber erteilt damit die Zustimmung (Autorisierung) zur Ausführung der Kartenzahlung. Zusätzlich können nach einem Zufallsprinzip bzw. risikobasiert die vom Karteninhaber während des Registrierungsprozesses hinterlegten persönlichen Daten (Sicherheitsfrage) abgefragt werden. Nach der Erteilung der Zustimmung kann der Karteninhaber die Kartenzahlung nicht mehr widerrufen.

4.2. App-Verfahren:
Beim App-Verfahren handelt es sich um ein Authentifikationsverfahren, bei welchem eine pro Mastercard Identity Check™- Transaktion generierte TAN via Internet direkt an eine besonders geschützte App auf das Smartphone des Karteninhabers übermittelt wird. Sobald eine Mastercard Identity Check™-Transaktion veranlasst wird, erhält der Karteninhaber auf seinem Endgerät eine Benachrichtigung. Nach Eingabe des App-Kennworts öffnet sich die App und die Transaktionsdetails sowie die pro Transaktion generierte TAN werden angezeigt. Durch Eingabe der erhaltenen TAN im Kaufprozess wird die Transaktion bestätigt und der Karteninhaber erteilt damit die Zustimmung (Autorisierung) zur Ausführung der Kartenzahlung. Nach der Erteilung der Zustimmung kann der Karteninhaber die Kartenzahlung nicht mehr widerrufen.

4.3. Die Nutzung der gesicherten Authentifizierung für Internetzahlungen kann für bestimmte Transaktionen zur Risikoprävention eingeschränkt sein.

5. Sorgfaltsanforderungen an den Karteninhaber

5.1. Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von Internetzahlungen Zugang zu seinem für das Verfahren genutzten Endgerät erlangt.

5.2. Das Endgerät, mit dem die TANs empfangen werden, darf nicht gleichzeitig für die Internetzahlungen genutzt werden (physische Trennung der Kommunikationskanäle).

5.3. Der Karteninhaber hat die Übereinstimmung der von MLP dem Nutzer übermittelten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und MLP zu informieren.

5.4. Der Karteninhaber hat die App nur aus offiziellen App Stores (Apple App Store oder Google Play Store) herunterzuladen und die für die App vorgesehenen Updates regelmäßig zu installieren.

5.5. Die Bank wird den Kunden nicht per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern. Jede Person, die die TAN kennt und in den Besitz der Karte kommt oder die Kreditkartennummer kennt, hat die Möglichkeit, zusammen mit der TAN und der Karte missbräuchliche Verfügungen zu tätigen (z. B. Zahlungsvorgänge über Internet bei Vertragsunternehmen veranlassen).

6. Änderung der Mobilfunknummer/virtuellen Handynummer

6.1. Sollte der Karteninhaber seine für das Verfahren genutzte Kennung (Mobilfunknummer für SMS-Empfang oder virtuelle Handynummer für App-Nutzung) ändern wollen, steht ihm auf der Registrierungswebseite der Bank eine Funktion zur Verfügung, um seine für das TAN-Verfahren verwendete Kennung zu ändern.

6.2. Ist kein TAN-Versand an die bisher registrierte Kennung möglich (z. B. wenn das Endgerät mit der hinterlegten Kennung gestohlen wurde), muss der Karteninhaber den Registrierungsprozess erneut durchlaufen.

7. Abmeldung vom Verfahren

7.1. Der Karteninhaber kann sich von der Teilnahme am Verfahren zur gesicherten Authentifizierung abmelden, indem er auf der Registrierungswebseite der Bank den Button „Benutzerdaten löschen“ betätigt.

7.2. Wenn sich der Karteninhaber abgemeldet hat, ist es ihm nicht mehr möglich, seine Kreditkarte für Internetzahlungen bei am gesicherten Authentifizierungsverfahren teilnehmenden Kartenakzeptanzstellen einzusetzen.
Um die Kreditkarte wieder bei diesen Kartenakzeptanzstellen einsetzen zu können, ist eine Neuregistrierung für Mastercard Identity Check™ erforderlich.

8. Datenerhebung und Datenverarbeitung, Einschaltung Dritter

8.1. Zur Durchführung und Abwicklung des Mastercard Identity Check™-Verfahrens bzw. einer Zahlung mit diesem Verfahren werden neben den genannten Daten zur Registrierung (siehe 3.) auch Daten aus der jeweiligen Transaktion erhoben und gespeichert. Dies erfolgt zur technischen Durchführung, zur Legitimationsprüfung, zur Zahlungsdurchführung und zur Betrugsprävention und umfasst insbesondere die verwendete Mobilfunknummer/virtuelle Handynummer, Angaben zu Zeitpunkt und Inhalt der authentifizierten Transaktionen inklusive Betrag und Plattform, versendete Nachrichten, Angaben zum Browser und Betriebssystem sowie gerätebezogene Angaben wie die IP-Adresse und Geräteidentifikationsnummer.

8.2. Die Bank ist berechtigt, sich zur Bewirkung der von im Rahmen des Mastercard Identity Check™-Verfahrens zu erbringenden Leistungen und zur Einforderung der vom Karteninhaber zu erbringenden Leistungen Dritter zu bedienen. Ist dafür die Verarbeitung von personenbezogenen Daten erforderlich, erfolgt dies im Auftrag und nach Weisung der Bank. Der Karteninhaber befreit die Bank gegenüber diesen Dienstleistern insoweit vom Bankgeheimnis.

8.3. Die Registrierungsdaten werden nach Beendigung des Kreditkartenvertrages entsprechend gesetzlicher Vorgaben aufbewahrt und nach Ablauf der Archivierungsfristen gelöscht. Die Transaktionsdaten werden zum Nachweis des Zahlungsvorganges gemäß gesetzlichen Vorgaben aufbewahrt und ebenfalls nach Ablauf der Archivierungsfristen gelöscht.

8.4. Nimmt eine Kartenakzeptanzstelle an dem Verfahren teil, übernimmt der jeweilige Dienstleister die Authentifizierung des Karteninhabers und teilt der Kartenakzeptanzstelle mit, ob der Authentifizierungsprozess erfolgreich war. Weitere Daten werden nicht an die Kartenakzeptanzstelle übermittelt. War der Authentifizierungsprozess nicht erfolgreich, wird der Authentifizierungsvorgang abgebrochen.

8.5. Die Bank verwendet die vom Karteninhaber für das Mastercard Identity Check™-Verfahren hinterlegte Rufnummer seines Mobiltelefons auch zur Kontaktaufnahme bei sicherheitsrelevanten Vorfällen bezüglich des Einsatzes seiner Kreditkarte (z. B. Verdacht auf Kartenmissbrauch durch Dritte). Dies beinhaltet auch die Verwendung der Rufnummer zur telefonischen oder elektronischen Abstimmung darüber, ob eine Transaktion auch tatsächlich vom Karteninhaber veranlasst wurde.

9. Haftung

9.1. Die Bank kann weder einen störungsfreien noch ununterbrochenen Zugang zur App gewährleisten.

9.2. Sie trägt keine Gewähr für die ständige Verfügbarkeit des Mastercard Identity Check™-Verfahrens und haftet nicht für Schäden infolge von Störung, Unterbrechungen (inkl. systembedingter Wartungsarbeiten) oder Überlastungen der beteiligten IT-Systeme.

9.3. Die Bank übernimmt keine Haftung bei Manipulationen des mobilen Endgerätes bzw. dessen Software, wie insbesondere einem sogenannten „Jailbreak" oder „Rooten" bzw. der Installation nicht vom Hersteller freigegebener Betriebssystemvarianten.

9.4. Die Bank haftet nicht für den Fall, dass das Endgerät verloren, gestohlen oder weitergegeben wird und dadurch Dritte Zugriff auf das vom Karteninhaber gewählte Verfahren zur gesicherten Authentifizierung erhalten und dieses ggf. unberechtigt nutzen.

10. Ablehnung von Kartenzahlungen durch die Bank

Die Bank ist berechtigt, die Kartenzahlung abzulehnen, wenn

- sich der Karteninhaber nicht mit der TAN legitimiert oder die weiteren persönlichen Daten genannt hat,
- der für die Kartenzahlung geltende Verfügungsrahmen der Karte oder die finanzielle Nutzungsgrenze nicht eingehalten ist oder
- die Karte gesperrt ist.

Hierüber wird der Karteninhaber über die Internetanwendung des Vertragsunternehmens, an dem die Karte eingesetzt wird, unterrichtet.

11. Änderungen der Bedingungen

Änderungen dieser Bedingungen werden dem Karteninhaber spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Karteninhaber mit der Bank im Rahmen seiner Geschäftsbeziehung einen elektronischen Kommunikationsweg vereinbart (z. B. das Online-Banking = MLP Financepilot), können die Änderungen auch auf diesem Weg angeboten werden. Die Zustimmung des Karteninhabers gilt als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat. Auf diese Genehmigungswirkung wird ihn die Bank in ihrem Angebot besonders hinweisen. Werden dem Kunden Änderungen dieser Bedingungen angeboten, kann er diese Geschäftsbeziehung vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen auch fristlos und kostenfrei kündigen. Auf dieses Kündigungsrecht wird ihn die Bank in ihrem Angebot besonders hinweisen.